REMARKS

Claims 14-28 and 37-44 are pending in this application, all of which stand rejected as a result of the August 10, 2005 Office Action. Claims 14-19, 21-28, and 37-44 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,718,361 (Basani) in view of U.S. Patent Application No. 2002/00022611 (Vange), and in further view of U.S. Patent No. 6,513,117 (Tarpenning). Claim 20 has been rejected under section 103(a) as being unpatentable over Basani as modified by Vange and Tarpenning in further view of U.S. Patent No. 6,425,017 (Dievendorff). Additionally, the Examiner has raised an issue under 37 C.F.R. § 1.48(a)(1). Applicants respectfully disagree with the grounds for rejection and traverse.

Inventor Statement under 37 C.F.R. § 1.48

The Examiner notes that Kathryn E. Hughes and Frank D. Byrum were added as inventors after the filing of this application. The Examiner further states that Ms. Hughes statement of lack of deceptive intent is on file, but Mr. Byrum's is not. Applicants have enclosed a copy of Mr. Byrum's statement – which was sent on November 5, 2002 and received by the Patent Office on November 14, 2002, at the same time as Ms. Hughes statement – along with a copy of the stamped postcard indicating the PTO's receipt of same. Applicants trust that the above-described documentation will resolve this issue.

The Section 103 Rejections

In response to a prior office action, applicants amended the independent claims to recite certain features relating to cryptography. At that time (in a paper filed on March 16, 2005), applicants argued, in essence, that none of the references that had been applied at that time (Basani, Vange, and Dievendorff) taught the cryptographic features recited in the claims. In particular, applicants argued: "... neither Vange nor Dievendorff explicitly mentions cryptography, and Basani mentions cryptography only in passing to note that standard cryptographic hash functions and ciphers exist. The use of cryptograph[y] – especially the particular types of items that are encrypted with particular keys, the

relationships between keys, and the features relating to which entities are aware of which keys, are not discussed at all in any of these references."

In response to applicants' argument, the Examiner has now cited a new reference (Tarpenning) for its alleged teaching of the various cryptographic features in the claims. While the section 103(a) rejections are based on a combination of the Basani, Vange, and Tarpenning references (as well as the Dievendorff reference, in the case of claim 20), the Examiner has relied entirely upon Tarpenning for the cryptographic features of the claims, and has not attempted to argue that the cryptographic features are present in any of the other references. Since the crux of the issue in this Office Action is whether Tarpenning teaches the cryptographic features recited in the independent claims, applicants will explain below why Tarpenning does not teach those features (although applicant notes, for the reasons stated above, that the other three applied references also do not teach or suggest the cryptographic features of the independent claims).

Independent Claim 14

Claim 14 recites various features concerning the use of three cryptographic keys (a "public key," a "first key," and "second key"). In particular:

- A "first server" generates a request that (1) represents the public key, and (2) is encrypted with the first key
- The first key is known to the first server and to a plurality of download servers, but is not known to a user
- A content item has (1) content encrypted with a second key, and (2) the second key encrypted by the public key.

In other words, there is a specified relationship between the public key, first key, second key, first server, plurality of download servers, and the user. Even if one can argue that Tarpenning teach the use of cryptography in general, Tarpenning does not teach the specific features recited in claim 14.

Tarpenning describes a "reader" that is associated with a "device public key" (see Tarpenning, col. 2, line 25 through col. 3, line 2). Additionally, a device on which a reader is installed can receive a "User Certificate" that "contains a different public/private key pair that will be used for decrypting content." (Tarpenning, col. 3, lines 10-12.) A user can then

purchase content for viewing with the reader (e.g., at a retail site, such as Amazon.com), and that content is typically received by the reader in an encrypted form. (See col. 4, ll. 52-55; col. 5, ll. 43-50.) When the content is received in an encrypted form, the encryption is "customized for the electronic ID of the particular reader ..., typically using the key or ID uniquely associated with that reader." (Col. 5, ll. 46-49.)

In arguing that Tarpenning teaches the features described in the bullet points above, the Examiner begins with the proposition that Tarpenning's alleged teaching of public/private keys corresponds to the claim feature of "a request comprising encrypted data that represents a public key associated with a user from whom said request is received and an identification of [a] content item." (For this feature the Examiner cites col. 3, ll. 8-22 of Tarpenning, which discusses a certificate that contains a public/private key.) Although the Examiner has not specifically explained how the cited portion of Tarpenning teaches the claim feature for which its is cited, the Examiner's position appears to be that the public key in the certificate corresponds to the "first key" recited in claim 14, and that the information that could be encrypted using Tarpenning's public key corresponds to the request. This argument suffers from various deficiencies, as described below.

First, if Tarpenning's certificate public key corresponds to the "first key" recited in the claim, then it is unclear what would correspond to the claimed "public key." As noted above, in claim 14 the "first key" is used to encrypt information representative of a "public key," and thus, in order to establish a correspondence between Tarpenning and the claimed invention, the Examiner would have to show a public key that is encrypted with a first key. (Of course, if the Examiner were to assert that Tarpenning's public key corresponds to both the first key and the claimed public key, then the Examiner would have to point to a portion of Tarpenning that shows the public key encrypting itself; applicants are not aware of any such teaching in Tarpenning. Also, the Examiner does not appear to have identified any portion of Tarpenning suggesting that the Tarpenning's certificate public key is encrypted by some other key. Thus, applicants assume that the Examiner's citation to the portion of Tarpenning describing the certificate public key is intended to mean that Tarpenning's certificate public key corresponds to the claimed "first key.".)

Second, if Tarpenning's public key corresponds to the "first key," then the information that is being encrypted with Tarpenning's public key (i.e., the "first key" in claim

14) must be a "request" that is received from a "first server." The Examiner appears to find that the "first server" is taught in col. 4, lines 52-60 of Tarpenning, which describes a transaction with a retail server, such as Amazon.com. In the sense of the Examiner's reasoning, the Amazon.com server fulfills the role of the "first server." However, in claim 14, the first server and the plurality of download servers both know the "first key," and the request is received from the "first server" and is encrypted with the first key. There is no suggestion in Tarpenning that Amazon.com (or any other retail site) shares knowledge of a first key with a plurality of download servers, or that a request encrypted by the first key (i.e., Tarpenning's certificate public key) is received from Amazon.com. In other words, the Examiner's analogy fails due to the fact that Tarpenning's certificate public key is not used in the manner recited in claim 14.

Third, we note that claim 14 calls for a content item to contain (1) content encrypted with a second key, and (2) the second key encrypted with the public key. With regard to this feature, the Examiner generally refers to steps 1105-1120 of Tarpenning, and asserts that the cited passage teaches that a "Revocation Token" is encrypted using an "Authentication Server Private Key, after which the result is encrypted using the Device Public Key." In other words, the cited portion of Tarpenning is asserted to teach that a token is doubly-encrypted with two keys, and the Examiner apparently finds this fact analogous to the claim feature of a "second key" encrypted with a "public key." As noted above, the Examiner has not stated what element in Tarpenning corresponds to the public key recited in the claim. However, if the Examiner's position is that Tarpenning's Revocation Token is encrypted constitutes the "second key," then – in order to maintain consistency between that position and the language of claim 14 – either the Authentication Server Private Key or the Device Public Key must correspond to the "public key" recited in claim 14, since claim 14 calls for the "second key" to be encrypted with the "public key." However, neither the Authentication Server Private Key nor the Device Public Key can constitute the public key mentioned in claim 14, since neither the Authentication Server Private Key nor the Device Public key is included in a request and encrypted with a "first key", as claim 14 calls for. (Recall that the Examiner has analogized the claimed "first key" to Tarpenning's certificate public key; it does not appear to be the case that the certificate public key is used to encrypt either the Authentication Server

Private Key or the Device Public Key; on the contrary, it appears that, in Tarpenning, the Device Public Key that is used to encrypt the certificate. See Tarpenning, col. 7, ll. 52-60.)

In summary, Tarpenning generally describes the use of cryptographic keys, but otherwise does not teach or suggest the specific features that claim 14 recites with respect to these keys. That is Tarpenning does not teach or suggest claim 14's features as to which keys are used to encrypt what information, or where the encrypted information is received, or which entities have knowledge of which keys. The rather specific structure and use of keys recited in claim 14 is designed to make it likely that certain information can pass from a first server to a download server through a user or a user's machine, but without the user being able to comprehend the information that is passed. (See Application, page 22, line 3 through page 23, line 7.) This structure cannot be inferred from Tarpenning, because Tarpenning uses keys in a different manner from the claimed invention. It cannot be said that one structure and usage involving keys (as described in Tarpenning) motivates an entirely different structure and usage of keys (as in claim 14).

Finally, for the reasons stated in applicants March 16, 2005, the other references cited (Basani, Vange, and Dievendorff) do not teach or suggest the cryptographic features recited in claim 14 – either alone, or in combination with Tarpenning.

For the foregoing reasons, applicants respectfully submit that claim 14 is patentable over the prior art, and request that the rejection of claim 14 be reconsidered and withdrawn.

Independent Claim 21

Independent claim 21 recites that there are a plurality of servers that share knowledge of a first key with a "first server" at which a request is generated. The request generated at the first server comprises a public key in a form encrypted by a first key. The public key is installed on a plurality of machines associated with a particular user. While claim 21 is not identical in scope or language to claim 14, it shares with claim 14 the common feature that there is a "first key" known to various servers but not to a user, and that the first key is used to encrypt a public key. As to these features relating to the use of cryptographic keys, the Examiner has applied the Tarpenning reference. As discussed above in connection with claim 14, Tarpenning does not teach or suggest that a public key is encrypted with a first key that is shared between specific servers but that is not shared with a user. Moreover, Tarpenning does

not teach or suggest that the public key in question is installed on a plurality of computers associated with a particular user. (In the portion of Tarpenning cited against the portion of claim 21 that addresses the public key being installed on a plurality of machine associated with a particular user, what Tarpenning actually shows in these cited portions is the certificate being installed on one particular machine. See Tarpenning col. 7, ll. 26-60.)

Thus, Tarpenning does not teach or suggest the features of claim 21 for which it is cited, and the applied prior art as a whole does not teach, suggest, or render obvious, claim 21. In view of the foregoing, applicants request that the rejection of claim 21 be reconsidered and withdrawn.

Independent Claim 37

Independent claim 37 recites that a request is received at one of a plurality of servers from a "remote" server; that the request comprises a public key associated with a user; that the request is encrypted with a first key; that the first key is known to the remote server and the plurality of servers, but not to the user; that a content item identified in the request is encrypted so as to be decryptable by with the first key; and that the first key is contained in the content item in a form decryptable with the public key.

While claim 37 is not identical to claims 14, and 21 in either language or scope, claim 37 recites features that are similar to some of the features relating to the use of keys discussed above in connection with claim 14. The Examiner has relied on Tarpenning for its alleged teachings of these features. For essentially the reasons discussed above in connection with claims 14 and 21, Tarpenning does not teach the particular use of keys recited in claim 37, and neither do any of the other applied references.

For the foregoing reasons, applicants request that the rejection of claim 37 be reconsidered and withdrawn.

Claim 16

Claim 16 is dependent on claim 14, and further recites that the user has engaged in a purchase transaction with a first server, where the first server includes functionality to determine whether to generate a request (or not to generate the request) depending on whether the user has completed said purchase transaction. In a prior Office Action, the

Examiner had relied on Vange as teaching this feature, and now relies on Tarpenning. For reasons previously stated in the March 16, 2005 paper, this feature is not found in Vange. Moreover, it is clear that this feature is not found in Tarpenning as applied. The Examiner has applied Tarpenning (col. 4, ll. 52-67) to the feature of claim 16 in question. However, that portion of Tarpenning describes a transaction with the amazon.com web site whereby a user purchases a book. There is no suggestion in the cited passage that Amazon.com either generates, or does not generate, a request depending on whether the user has completed a purchase transaction. Rather, in the Tarpenning's description of the book-purchase transaction, it appears that the user receives the book only if he or she has paid for the book. However, sending the user a book is not the same thing as generating a request, because the book itself is not the same thing as a request for the book.

Accordingly, the newly-cited Tarpenning reference fails to teach the features of claim 16, and does not address the deficiency in the prior Office Action's reliance on Vange. Accordingly, applicants requests that the rejection of claim 16 be reconsidered and withdrawn.

Claims 19 and 24

While claims 19 and 24 are not identical in either language or scope, both of these claims recite limits as to the number of machines on which a public key associated with a user can be installed.

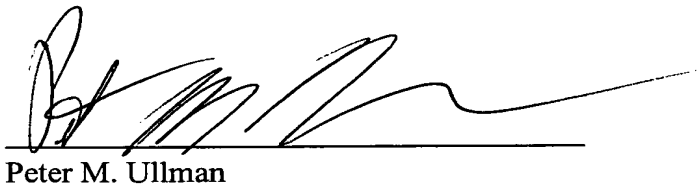
As to these features, the Examiner has relied on Tarpenning – in particular, col. 7, line 60 through col. 8, line 5. This portion of Tarpenning describes the process to install a user certificate. In general, each certificate is assigned a sequence number and – as one type of check to determine whether the certificate should be installed on a particular machine – the server performing the installation verifies that the sequence number of the certificate that is about to be installed is greater than the sequence number of a prior certificate on the target machine. The presumption in Tarpenning is that, if the sequence number of the certificate to be installed is lower than the sequence number of the previously-installed certificate, then it is possible that the certificate is being installed on the wrong machine, since sequence numbers should go up, rather than down. However, this use of sequence numbers has nothing to do with a limit *as to the number of machines on which a public key can be installed.*

Tarpenning's process of checking that the sequence numbers increase does not impose a limit on the number of machines on which a certificate can be installed. In Tarpenning, a certificate can be installed as long as the sequence number of the new certificate is greater than the sequence number of the last certificate. Since the numbers can increase up to an infinite number, there is no limit in Tarpenning as to how many times the certificate can be installed, as long as the sequence numbers of the certificate continue to increase.

Thus, the sequence number feature of Tarpenning does not teach or suggest the features of claims 19 and 24 for which it is cited. Applicants thus request that the rejection of claims 19 and 24 be reconsidered and withdrawn.

Conclusion

Claims 14, 16, 19, 21, 24, and 37 have been shown to be patentable over the applied prior art, and claims 15, 17, 18, 20, 22, 23, 25-28, and 38-44 are patentable at least by reason of their dependency. All issues having been addressed, applicants respectfully submit that this case is now in condition for allowance.



Date: November10, 2005

Peter M. Ullman
Registration No. 43,963

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Marco A. DeMello, Pavel Zeman, Vinay Krishnaswamy, and Prashant Malik

Group Art Unit: 2782

Examiner: Not Yet Assigned

Serial No.: 09/604,939

Filed: June 27, 2000

For: ASYNCHRONOUS COMMUNICATION WITHIN A SERVER ARRANGEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

STATEMENT IN SUPPORT OF PETITION TO CORRECT INVENTORSHIP UNDER 37 C.F.R. ' 1.48(a)

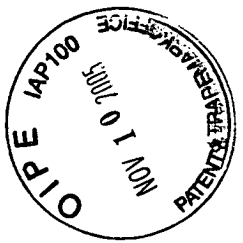
I, **Frank D. Byrum**, state that:

1. An error in inventorship exists in the above-identified patent application.

2. The error arose because the above-identified application inadvertently did not list me as an inventor.

3. I understand that, to correct this error, I am being added as an inventor.

4. This error in inventorship occurred without deceptive intention on my part.



I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this statement is directed.

Date: 21 Aug 2002

Frank D. Byrum

RECEIVED BY THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Paper: **Amendment, Request and Processing Fee** to Add to Delete, and/or Add to Original Erroneously Named or Not Named Inventor(s) in Declaration – Nonprovisional Application – (37 CFR 1.48(a)) (w/first class certification); Two (2) **Statements in Support** of Petition to Correct Inventorship Under 37 C.F.R. 1.48(a) – (for Kathryn E. Hughes and Frank D. Byrum); **Executed Declarations and Powers of Attorney** for Marco A. DeMello, Pavel Zeman; Vinay Krishnaswamy; Prashant Malik; Kathryn E. Hughes;and Frank D. Byrum, **Consent of Assignee** to Change of Inventorship in Patent Application; **Statement Under** 37 CFR 3.73(b); Check for $130 processing fee; return postcard

Applicant(s) :Marco A. DeMello, *et al.*

Title: Asynchronous Communication Within a Server Arrangement
Serial No.: 09/604,939
Filed: June 27, 2000

Docket No.: MSFT-0186/154572.1
Date Sent: **November** 05, 2002 **Sent By:** PMU/R. Ader